ORIGINAL BY FAX

DAVID C. PARISI (SBN 162248)
(dparisi@parisihavens.com)
SUZANNE HAVENS BECKMAN (SNB 188814)
(shavens@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818)990-1299
dcparisi@msn.com

JAY EDELSON
(jedelson@kamberedelson.com)
MICHAEL J. ASCHENBRENER
(maschenbrener@kamberedelson.com)
CHRISTOPHER L. DORE
(cdore@kamberedelson.com)
BENJAMIN H. RICHMAN
(brichman@kamberedelson.com)
KAMBEREDELSON, LLC
350 North LaSalle Street
Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
Fax: (312) 589-6378

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

E-filing

RS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

C 09 6032

ALAN CLARIDGE, an individual, on behalf of himself and all others similarly situated, Plaintiff, v. ROCKYOU, INC., a Delaware corporation, Defendant.	Case No. **CLASS ACTION COMPLAINT FOR:** **(1) Violations of Cal. Bus. & Prof. Code § 17200** **(2) Violations of Cal. Penal Code § 502** **(3) Violations of Cal. Civ. Code § 1798.80** **(4) Violations of Cal. Civ. Code § 1750** **(5) Breach of Contract** **(6) Breach of Implied Contracts** **(7) Breach of the Implied Covenant of Good Faith and Fair Dealing** **(8) Negligence** **(9) Negligence Per Se** **DEMAND FOR JURY TRIAL**

Plaintiff, by and through his attorneys, upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff, Alan Claridge ("Claridge"), brings this class action complaint against RockYou, Inc. ("RockYou") for failing to secure and safeguard its users' sensitive personally identifiable information ("PII"), including e-mail addresses and passwords, as well as login credentials for social networks such as MySpace and Facebook. RockYou knowingly stored Plaintiff and the Class members' PII in an unprotected format and in a manner easily accessible to malicious intruders, in violation of its own Privacy Policy and accepted industry standards.

2. RockYou is a publisher and developer of popular online applications and services for use with social networking sites such as Facebook, MySpace, hi5 and Bebo.

3. RockYou stored users' PII in an unencrypted database with poor network security. RockYou's willful failure to secure its users' sensitive PII led to multiple security breaches that exposed 32 million users to identity theft and other malicious conduct. While some security threats are unavoidable in a rapidly developing technological environment, RockYou recklessly and knowingly failed to take even the most basic steps to protect its users' PII by leaving the data entirely unencrypted and available for any person with a basic set of hacking skills to take the PII of at least 32 million consumers.

PARTIES

4. Plaintiff Alan Claridge is a resident of Evansville, Indiana. He is a registered user of RockYou, Inc.'s services.

5. Defendant RockYou, Inc. is a California corporation headquartered in San Mateo County, California, at 585 Broadway Street, #A, Redwood City, California 94063. RockYou does business throughout the State of California and the nation.

JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because (a) at lease one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

7. Personal jurisdiction and Venue are proper because RockYou is a corporation headquartered in San Mateo County and/or because the improper conduct alleged in the Complaint occurred in, was directed from, and/or emanated or exported from California.

INTRADISTRICT ASSIGNMENT

8. Pursuant to Local Civil Local Rule 3-2(d), this case shall be assigned to either the San Francisco or Oakland Division.

FACTS

9. RockYou offers a variety of products for use through online social networks such as Facebook and MySpace. These products include applications to share photos, write special text on a friend's page, or play games with other users. Once a user begins operating a RockYou application on a social network site, RockYou utilizes that application as a platform to display paid advertisements. RockYou claims to be the leading provider of social networking application-based advertising services, with more than 130 million unique customers using its applications on a monthly basis.

10. A customer may sign up to use RockYou's applications through rockyou.com by providing a valid e-mail address and a registration password. RockYou then stores this e-mail address and password in a database. Additionally, and depending upon which online social network a customer chooses to utilize RockYou's products, a user may be required to provide RockYou with a username and password for accessing that network. RockYou also stores this information in its database.

11. RockYou asserts through its website that it will safeguard its users sensitive PII. RockYou's Privacy Policy specifically states:

> Our Commitment To Data Security: RockYou! uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you transmit to RockYou! and you do so at your own risk. Once we receive your transmission of information, RockYou! makes commercially reasonable efforts to ensure the security of our systems….

12. Plaintiff and the Class agreed to RockYou's Terms of Use and Privacy Policy in order to register and use RockYou's products.

RockYou's Unencrypted and Unprotected Storage of PII

13. Under its user agreements, RockYou collects and stores millions of users' PII on a large-scale commercial database, claiming to use "commercially reasonable" methods of data protection. However, until approximately December 5, 2009, RockYou's database stored users' PII in "clear" or "plain" text, meaning there was no form of encryption preventing an intruder from easily reading and removing the sensitive PII. Under widely accepted standards, storing users' PII in clear text is fundamentally outside the bounds of modern database security and a significant risk to the integrity of a user's PII.

14. Clear text passwords are not stored in a cryptographically protected form, and therefore are readily accessible to anyone with access to the database. This means that once a hacker gains access to a network or database system, there is no further barrier or protection to removing e-mail addresses and passwords as they are presented without encryption or additional security. Those with access – authorized or unauthorized – may read the passwords as easily as one can read the words in this Complaint.

15. By way of analogy, a properly protected database could be compared to the safety deposit box room at a bank. At any major bank, the hundreds of safe deposit boxes are

found inside a walk-in-safe, but then additionally protected by individual two-key locked doors. In the website context, the outer safe door represents basic network security that prevents a hacker from getting anywhere close to a database. However, in the event that a thief is able to bypass the outer safe door, he will encounter a significant second layer (or more) of security to thwart his intentions. RockYou not only left the outer safe door entirely open (as detailed below), but also, left the individual safety deposit boxes open with their contents on display.

16. Among the options available to protect its customers' PII, RockYou could have followed a commonly used method of protecting sensitive data that requires conversion and storage of a "hashed" form of a plain text password.[1] A properly designed hash function will make it virtually impossible to decipher the original plain text password.

17. RockYou failed to use hashing, salting, or any other common and reasonable method of data protection and therefore drastically exacerbated the consequences of a hacker bypassing its outer layer of web security.

Consumers' E-Mail and Password Unlocks Endless Amounts of Sensitive PII

18. The information stored in RockYou's user database is a very powerful set of PII, including email login credentials, that may be used for damaging and malicious purposes.

19. By failing to secure its users' PII, RockYou made all of this data available to even the least capable hacker.

---

[1] Under this method, when a user inputs a password, the software runs through a cryptographic hash algorithm, and if the hash value generated from the user's input matches the hash stored in the database, access is permitted. A hash value is created by applying a hash function to a string consisting of the submitted password and another value known as a "salt." The salt prevents attackers from easily building a list of hash values for common passwords.

20. Because a majority of internet users utilize identical passwords across a wide range of websites, gaining access to a user's e-mail account name and password has a high likelihood of providing access to a users' personal and/or work e-mail account.[2]

21. Because a person's e-mail account acts as a modern day file cabinet for a variety of interactions, transactions, and correspondence, and is fully searchable, even a cursory review of personal e-mails can provide a litany of valuable and compromising information.

22. For example, once a hacker accesses a users' e-mail account, he may be able to take any of the following actions:

a. Extract private information from the e-mail inbox including credit card numbers, confidential business information, bank account numbers, etc.;

b. Easily see where that person transacts business online (*e.g.*, purchases from online retailers such as Amazon.com or e-mails from a person's bank). Once a person can see where a consumer transacts business, it allows them to (1) attempt to use the e-mail and password already in their possession to sign into that account; or (2) utilize a website's built in "forgotten password" reset mechanism to send a new password to the now accessible e-mail account. Once signed into an online retailer, a consumer's credit card is often pre-stored and may be used for a purchase;

c. Access an online payment service such as PayPal, which allows a person to make purchases through a pre-linked credit card;

d. Achieve a full scale identify theft by accessing a consumer's social security number, phone number, home address, tax information, bank or credit card account number, birth date, etc.;

e. Access health insurance information (including account numbers and

---

[2] *See* Rob Leathern, *FTC Security Workshop, Security and Privacy Data*, May 20, 2002 (finding that over fifty percent of web users use identical passwords across all websites and applications).

passwords), medical records, and otherwise private and confidential medical information;

f. Harvest the consumer's contact list for spam. Assuming that each of the exposed 32 million e-mail accounts has only 10 unique contacts (a dramatically conservative estimate), a spammer will have 300 million live e-mail addresses to spam, as well as any phone numbers contained in a user's contact information to use for spam text messages or for use in illegal phone bill cramming.

The Attack on RockYou's Database

23. On December 4, 2009, the online security firm Imperva, Inc. notified RockYou of a security problem with its SQL database.[3] Imperva specifically informed RockYou that it had become aware of a SQL injection flaw[4] as a result of monitoring underground hacker forums. According to Imperva, hackers were regularly discussing RockYou's SQL injection vulnerability and the fact that it was being actively exploited.

24. SQL injection flaws have consistently been among the top online security problems of the past decade. For example, in 2007 and 2008, hackers took advantage of a SQL injection flaw to steal 130 million credit card numbers stored on the databases of Heartland Payment Systems, 7-Eleven, and Hannaford Brothers. The attack was widely publicized and is regarded as the largest case of identity theft in American history, re-emphasizing the danger SQL injection attacks pose to commercial database security.

25. Because knowledge and understanding of SQL injection flaws has been widespread for more than a decade, measures for protection have become readily available.

---

[3] Like thousands of commercial website operators who collect user information, RockYou utilizes a Structured Query Language ("SQL" (pronounced "sequel")) database. SQL is a database computer language designed for storing data in relational database management systems such as when a company needs to store and manage millions of e-mail accounts and passwords.

[4] A SQL injection flaw allows a hacker to take advantage of improperly coded web software to introduce malicious code into a company's network. A hacker may capitalize on the improperly coded software to send a malformed SQL query to the underlying database to break into it, plant malicious code or access other systems on the network.

SQL injections flaws, therefore, are relatively easy to prevent and are well known to any web developer handling a large-scale commercial website.

26. Based on its own findings, Imperva believed that prior to warning RockYou, it was likely that breaches had already occurred through RockYou's SQL injection flaw. Additionally, Imperva informed RockYou that its researchers were aware that RockYou users' webmail accounts had been accessed as a result of prior breaches.

27. The SQL injection flaw was disproportionally hazardous to RockYou's users because RockYou had failed to encrypt its users' PII. Therefore, once a hacker got inside RockYou's network, there was no further deterrent or obstacle to stealing RockYou's users' PII.

28. Had RockYou properly secured its database through known and available encryption methods, and even if a hacker were able to enter the network, he would be limited in his ability to inflict harm. For example, a hacker still might be able cause temporary internal havoc in the operation of the site, or "vandalize" the appearance of the site by altering its code, but under the appropriate and necessary security, a hacker would not be able to steal 32 million sets of user PII because the data would be encrypted and indecipherable.

29. However, because RockYou did not have this security in place, RockYou's security flaw was being actively exploited and the contents of its database were known and made public through underground hacker forums on or before November 29, 2009

30. In a December 15, 2009, interview conducted by SCMagazineUS.com, Imperva's chief technology officer, Amichai Shulman, reports:

> Others probably hacked into the database even earlier, Shulman said. Imperva researchers initially discovered the vulnerability after coming across a thread on a hacking forum, where hackers discussed the flaw and said it was being actively exploited.
>
> "It was probably compromised before we warned them about it," Shulman said. He added that Imperva researchers are

> certain that some webmail accounts have been accessed as a result of the breach.
>
> "I can tell you for sure that some of them have been accessed," Shulman said. "We know that for a fact. We looked at some of those accounts and they were already flagged as abused by the webmail providers."
>
> "SQL injection is one of the oldest tricks in the book of application-level hacking and it allows direct access to the database through the web app," Shulman said.[5]

31. Based on RockYou's own press release, after Imperva warned it of the SQL injection vulnerability and the high likelihood of prior breaches, RockYou "immediately brought down the site and kept it down until a security patch was in place."[6]

32. However, RockYou did not in fact respond immediately to the warning and waited at least one day to take action to repair the SQL vulnerability. According to an interview conducted by NetworkWorld.com with Imperva's chief technology officer, Amichai Shulman, "RockYou did not respond to Imperva, nor did it appear to immediately take down its site as it claimed in its statement to Tech Crunch, Shulman said. The flaw was present for a day or more after Imperva informed RockYou of the issue before it was addressed he said."[7]

33. In the time prior to RockYou fixing the SQL vulnerability, at least one confirmed hacker known by the moniker "igigi" accessed RockYou's database and removed the e-mails and passwords of approximately 32 million registered RockYou users.

34. This hacker accessed and removed the user information prior to Imperva's warning, and therefore entered RockYou's database without detection. Further, by entering the database prior to Imperva's warning, the hacker acted with separate and independent knowledge of RockYou's vulnerability.

---

[5] http://www.scmagazineus.com/rockyou-hack-compromises-32-million-passwords/article/159676/

[6] http://www.techcrunch.com/2009/12/14/rockyou-hacked/

[7] http://www.networkworld.com/news/2009/121509-rockyou-hack-exposes-names-passwords.html?page=1

35. In an interview with RockYou's Chief Technology Officer, Jia Shen, Digital Beat reported that after Imperva notified RockYou of its security vulnerability, "the company began poring through its databases to find any evidence of attack. Shen said the company doesn't know exactly what the hacker did in the attack. The company is in contact with law enforcement but isn't saying more. 'But we are assuming the worst,' Shen said. 'We checked the activity and it looked like it had been going on a couple of days before we were warned.' Mr. Shen continued, 'We started off as a small company and today we have a different engineering structure,' he said. 'But shame on us. If you make a mistake, then people can get in and it is a big hole.'"[8]

36. On information and belief, the "activity" referred to by Mr. Shen was in fact not the individual hacker known as "igigi" who publically claimed to have accessed the database, but one or more different individuals.

37. On information and belief, RockYou did not utilize any software designed to identify actual or potential attacks, forcing RockYou to manually search for attacks after they had occurred.

38. In a statement issued after RockYou publically announced the security breach, RockYou stated that "one or more individuals illegally breached one of our databases that contained the usernames and passwords for about 32 million users in an unencrypted format." While RockYou indicated that updates and increased security were put in place following the breach, it acknowledged that at the time of the breach, the hacked database had not been up-to-date with regard to "industry standard security protocols."[9]

39. Implicit in RockYou's statement is the admission that the security methods it utilized to protect user PII did not meet even the most basic industry standards and recklessly exposed its users' information to attack and theft.

---

[8] http://digital.venturebeat.com/2009/12/15/rockyou-explains-how-a-hacker-stole-32-million-passwords-and-what-its-doing-about-it/

[9] http://www.rockyou.com/help/securityMessage.php

FACTS RELATING TO PLAINTIFF

40. During the relevant time period, Alan Claridge was a registered account holder with RockYou. He registered with RockYou on August 13, 2008.

41. In signing up to utilize a photo sharing application offered by RockYou, Claridge submitted his e-mail address and a password to RockYou.

42. On December 16, 2009, Claridge received an e-mail from RockYou informing him that his sensitive PII stored with RockYou may have been compromised through a security breach.

CLASS ALLEGATIONS

43. Plaintiff Alan Claridge brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of himself and a Class of similarly situated individuals, defined as follows:

> All individuals and entities in the United States who registered an account with RockYou, Inc.

Excluded from the Class are Defendant, its legal representatives, assigns, and successors, and any entity in which Defendant has a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family, as well as any individual who contributed to the unauthorized access of RockYou's database.

44. The Class consists of millions of individuals and other entities, making joinder impractical.

45. Plaintiff's claims are typical of the claims of all of the other members of the Class.

46. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the

financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

47. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

48. RockYou has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class.

49. The factual and legal bases of RockYou's liability to Plaintiff and to the other members of the Class are the same and resulted in injury to Plaintiff and all of the other members of the Class. Plaintiff and the other members of the Class have all suffered harm as a result of RockYou's wrongful conduct.

50. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

(a) whether RockYou failed to use reasonable care and utilized commercially reasonable methods to secure and safeguard its users' sensitive PII;

(b) whether storing user e-mails and passwords in an unencrypted format was commercially reasonable;

(c) whether RockYou's conduct described herein violated the Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*);

(d) whether RockYou's conduct described herein violated California's Computer Crime Law (Cal. Penal Code § 502);

(e) whether RockYou's conduct described herein violated the California Security Breach Information Act (Cal. Civ. Code § 1798.80, *et seq.*);

(f) whether RockYou's conduct describe herein violated the California Legal Remedies Act (Cal. Civ. Code § 1750);

(g) whether RockYou's conduct described herein constitutes a breach of contract;

(h) whether RockYou's conduct described herein constitutes breach of the implied covenants of good faith and fair dealing;

(i) whether RockYou's conduct described herein constitutes breach of implied contracts;

(j) whether RockYou's conduct described herein was negligent and/or grossly negligent;

(k) whether RockYou's conduct described herein constitutes negligence per se;

51. Plaintiff reserves the right to revise these definitions based on facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

52. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

53. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

54. The UCL prohibits any unlawful, unfair or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair

competition. An unlawful business practice is anything that can properly be called a business practice and that at the same time is forbidden by law.

55. As described herein, Defendant's failure to safeguard and secure its users' sensitive PII and permit it to be stolen is a violation of the UCL.

56. Commonly accepted and widely practiced industry standards provide that sensitive PII stored in a commercial database should be not be accessible to theft or manipulation through a SQL injection attack, and commercially reasonable methods to prevent such attacks are widely known throughout the security industry. Further, commonly accepted and widely practiced industry standards provide that sensitive PII stored in a commercial database, especially user passwords, should be not be stored in "clear" text, but rather encrypted to provide a barrier to removal or manipulation.

57. RockYou failed to expend the resources necessary to protect the sensitive data entrusted to it by Plaintiff and the Class in clear contradiction of accepted industry standards for database security. In creating the perception that it followed industry standards for database protection, RockYou gained an unfair advantage over its competitors.

58. Additionally, RockYou deceived consumers by providing in its Terms of Use that it "uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information….Once we receive your transmission of information, RockYou! makes commercially reasonable efforts to ensure the security of our systems."

59. RockYou's failure to develop its online software applications in a manner resistant to SQL injection attacks, and/or monitor its database systems for SQL injection flaws, is not a "commercially reasonable" method of preserving the integrity of user information.

60. RockYou's failure to maintain an encrypted database of user e-mails and passwords is not a "commercially reasonable" method of preserving the integrity of user

information. Storing sensitive PII in clear text provides no level of data security and significantly increases the likelihood of data theft.

61. Maintaining sensitive PII with substandard security, when reasonable additional security is not only available, but allegedly in use within other parts of RockYou's computer system, is not a "commercially reasonable" method of preserving the integrity of user information.

62. Defendant has violated the "unlawful" prong of the UCL in that Defendant's conduct violated the Consumer Legal Remedies Act (Cal. Civ. Code § 1750 *et seq.*), the California Computer Crime Law (Cal. Penal Code § 502), and the California Security Breach Information Act (Cal. Civ. Code § 1798.80, *et seq.*).

63. Defendant has violated the fraudulent prong of the UCL in that Defendant misrepresented to its users that it would use commercially reasonable methods to safeguard and secure their PII and induce them to use its services and entrust it with their sensitive data.

64. Defendant has violated the unfair prong of the UCL in that Defendant operated a business that induced consumers to submit PII with the written assurance that it would be protected through commercially reasonable methods. Defendant knowingly failed to provide any commercially reasonable security methods and allowed its users' PII to be stolen by malicious third parties.

65. Defendant's unfair or deceptive practices occurred primarily and substantially in California. Decisions concerning the retention and safeguarding of user information were made in California, RockYou maintains all or a substantial part of its computer systems containing user information in California, and the security breach of its computer systems took place primarily and substantially in California.

66. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff seeks an order of this Court permanently enjoining Defendant from continuing to engage in the unfair and unlawful conduct described herein. Plaintiff seeks an order requiring Defendant to (1) immediately

stop the unlawful practices stated in this Complaint; (2) pay attorney's fees, and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SECOND CAUSE OF ACTION
Violation of California's Computer Crime Law ("CCCL")
Cal. Penal Code § 502,
(On Behalf of Plaintiff and the Class)

67. Plaintiff incorporates the foregoing allegations as if fully set forth herein. RockYou knowingly and without permission provided a means for a malicious third party to access its database and alter, damage, delete, destroy, steal, copy or otherwise use its users' data in violation of Cal. Penal Code § 502(c)(6).

68. RockYou knowingly and intentionally failed to follow even the most basic database security protocols and thereby failed to safeguard and secure its users' sensitive PII, allowing that information to be manipulated and stolen by a third party.

69. RockYou's reckless indifference to the proper security measures necessary to protect its users' sensitive PII created the gaping security hole necessary for a malicious third party to directly access its database. Without RockYou's reckless and/or gross negligence and unwillingness to follow industry standards for data security, a third party hacker could not have stolen Plaintiff and the Class's sensitive PII.

70. As a direct and proximate result of RockYou's violation of § 502, RockYou caused loss to Plaintiff and the Class members in an amount to be proven at trial. Plaintiff and the Class are entitled to the recovery of attorneys' fees pursuant to § 502(e).

71. Plaintiff and Class members have also suffered irreparable injury as a result of Defendant's unlawful conduct, including the harvesting of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiff and the Class have no adequate remedy at law, entitling them to injunctive relief.

THIRD CAUSE OF ACTION
Violation of the California Security Breach Information Act
Cal. Civ. Code § 1798.80, *et seq.*
(On Behalf of Plaintiff and the Class)

72. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

73. From 2006 through the present, RockYou conducted business in the State of California and maintained a database of computerized data that included sensitive PII.

74. As of December 4, 2009, at the very latest, RockYou was notified and given substantial grounds to reasonably believe that its database was the subject of a substantial security breach that resulted in an unauthorized third party acquiring its users' personal information. RockYou did not give complete and proper notice of any security breach until 10-12 days later, and only after significant media attention.

75. By waiting at least 10 to 12 days to provide notice of the breach to its users, RockYou failed to act in a timely fashion, thereby delaying Plaintiff and the Class's ability to protect their personal information from the multiple security breaches, including but not limited to the security breach perpetrated by the hacker known as "igigi," and all other security breaches Imperva warned RockYou about. Because of RockYou's willful ignorance and unwillingness to provide even the most basic forms of database and network security, it failed to detect any type of security breaches and/or SQL injection attacks until after it was informed of its vulnerabilities, and even then, failed to take timely action to protect its users' information.

76. RockYou did not give notice of any potential security breach in the most expedient time frame possible and was unreasonably delayed responding to the breach.

77. Separate from any unidentified security breaches, RockYou did not publicly post a warning notice on its website regarding the vulnerability and possible attacks on December 15, 2009, even though it was given a warning and aware of its issues on December 4, 2009 at the latest. The public notice only appeared after significant media coverage and a

direct threat from the hacker known as "igigi." The public notice only appears on RockYou's front page, and not on an individual's profile page, the actual web page that registered users use to create and manage RockYou products.

78. Likewise, RockYou failed to individually give notice to all of its users until at least December 15 or 16, 2009, when it sent the following e-mail to its users:

> Dear RockYou user,
>
> As you know, RockYou takes our users privacy very seriously. We take a lot of effort to protect user data from security breaches and attacks.
>
> Unfortunately, RockYou has very recently learned that it encountered a security breach. As part of this breach, it is possible that someone may have accessed at least your email address and password for the RockYou system. We felt it was important to notify you of this immediately so that you could take any action you feel necessary to protect your privacy.
>
> As a precaution, we strongly recommend you change any passwords for other online websites that have the same login and password immediately in order to protect your security.
>
> If you have any questions, please feel free to contact security@rockyou.com. We are sorry for any problems this has caused you.
>
> The RockYou team

79. This e-mail was therefore issued at least 12 days after RockYou was notified of the security vulnerability, and only after receiving significant media attention and pressure.

80. This notice fails to conclusively inform its users that their data has been stolen as a result of the breach, which RockYou was more than aware of by this time. Therefore, the notice is not only untimely, but insufficient.

81. Under Cal. Civ. Code § 1798.84, Plaintiff and the Class seek damages, all applicable civil penalties, and reasonable attorneys' fees and costs.

FOURTH CAUSE OF ACTION
Violation of the Consumers Legal Remedies Act
Cal. Civ. Code § 1750, *et seq.*
(On Behalf of Plaintiff and the Class)

82. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

83. The Consumers Legal Remedies Act prohibits the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, concealment, suppression or omission of any material fact with intent that others rely upon such act in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

84. As described within, Defendant has engaged in deceptive practices, unlawful methods of competition, and/or unfair acts as defined by Cal. Civ. Code §§ 1750, *et seq.*, to the detriment of Plaintiff and the Class.

85. Defendant, acting with knowledge, intentionally and unlawfully brought harm upon Plaintiff and the Class by deceptively inducing Plaintiff and the Class to register with RockYou based upon deceptive and misleading representations that it would take commercially reasonable steps to safeguard its users' sensitive PII. Specifically, Defendant violated Cal. Civ. Code § 1750 in at least the following respects:

(a) In violation of § 1770(5) by representing that goods or services have characteristics and benefits, which they do not have;

(b) In violation of § 1770(a)(19) by inserting an unconscionable provision in the offer for Defendant's goods and services.

86. Plaintiff and the Class have suffered harm as a direct and proximate result of the Defendant's violations of law and wrongful conduct.

87. Under Cal. Civ. Code § 1780(a) and (b), Plaintiff and the Class seek injunctive relief requiring Defendant to cease and desist the illegal conduct described herein, and any other appropriate remedy for violations of the CLRA. For the sake of clarity, Plaintiff explicitly disclaims any claim for damages under the CLRA at this time.

FIFTH CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

88. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

89. In order to use its social-networking applications, Defendant required that Plaintiff and the Class affirmatively assent to its Terms of Use Agreement (the "Agreement").

90. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff and the Class on the one hand, and Defendant on the other.

91. Under the Agreement, in order to use Defendant's social networking applications, Plaintiff and the Class transmitted several pieces of sensitive PII to Defendant, including but not limited to their e-mail addresses and corresponding passwords. In turn, under the Agreement Defendant promised that "RockYou! uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information." Defendant further promised that it would provide Plaintiff and the Class with prompt and sufficient notice if their sensitive PII was compromised.

92. Defendant materially breached the terms of the Agreement by its wrongful conduct alleged herein, including failing to properly secure its databases, thereby allowing Plaintiff's and the Class's sensitive PII to be compromised. Defendant further materially breached the terms of the Agreement by failing to promptly and sufficiently notify Plaintiff and the Class that their sensitive personal information had been compromised.

93. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff and the Class suffered injury.

SIXTH CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

95. In order to use Defendant's social-networking applications, Plaintiff and the Class affirmatively assented to Defendant's Terms of Use Agreement.

96. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff and the Class on the one hand, and Defendant on the other.

97. Implicit in the Agreement were contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiff's and the Class's rights to receive the benefits of the Agreement.

98. Defendant's obligation to take commercially reasonable steps to safeguard and secure Plaintiff's and the Class's sensitive PII from unauthorized access and theft was a material term of the Agreement. Equally material was Defendant's obligation to provide prompt and sufficient notice to Plaintiff and the Class in the event that their sensitive PII had been compromised.

99. Furthermore, implicit in the terms of the Agreement was Defendant's obligation to comply with Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Cal. Penal Code § 502, Cal. Civ. Code §§ 1798.80, *et seq.*, and Cal. Civ. Code §§ 1750, *et seq.*

100. Defendant breached the implied covenant of good faith and fair dealing by failing to safeguard and secure Plaintiff's and the Class's sensitive PII from unauthorized access and theft, failing to promptly and sufficiently notify Plaintiff and the Class that their sensitive PII had been compromised, and further by failing to fully comply with the proscriptions of applicable statutory law.

101. Defendant's misconduct and breach of the implied covenant of good faith and fair dealing as described herein resulted in injury to Plaintiff and the Class.

SEVENTH CAUSE OF ACTION
Breach of Implied Contracts
(On Behalf of Plaintiff and the Class)

102. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

103. In order to use Defendant's social-networking applications, Plaintiff and the Class transmitted several pieces of sensitive PII to Defendant, including their e-mail addresses and corresponding passwords.

104. By providing that sensitive PII and upon Defendant's acceptance of such information, Plaintiff and the Class, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take commercially reasonable steps to secure and safeguard that information.

105. Under the implied contract, Defendant was further obligated to provide Plaintiff and the Class prompt and sufficient notice of any and all unauthorized access and/or theft of their sensitive PII.

106. Without such implied contracts, Plaintiff and the Class would not have provided their personal information to Defendant.

107. By failing to properly secure Plaintiff's and the Class's sensitive PII, and further by failing to notify Plaintiff and the Class that their personal information had been compromised, Defendant breached its implied contracts with Plaintiff and the Class.

108. Defendant's breach and other misconduct described herein resulted in injury to Plaintiff and the Class.

EIGHTH CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

109. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

110. In order to use Defendant's social-networking applications, Plaintiff and the Class transmitted several pieces of sensitive PII to Defendant, including their e-mail addresses and corresponding passwords.

111. By agreeing to accept Plaintiff's and the Class's sensitive PII, Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so.

112. Defendant failed to protect its databases against SQL injection attacks and other security vulnerabilities, failed to encrypt Plaintiff's and the Class's passwords, and failed to provide Plaintiff and the Class with prompt and sufficient notice that their sensitive PII had been compromised, thereby breaching its duties to Plaintiff and the Class.

113. By failing to take proper security measures to protect Plaintiff's and the Class's sensitive PII as described herein, Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

114. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, its databases were accessed without authorization and Plaintiff's and the Class's sensitive PII was compromised.

115. That security breach and resulting unauthorized access to Plaintiff's and the Class's sensitive PII was reasonably foreseeable by Defendant, particularly in light of the fact that the method used to access Defendant's databases—an SQL injection attack—was well-known within the industry and had been successfully guarded against by companies similar to Defendant for approximately a decade prior to the instant breach.

116. Neither Plaintiff nor the other members of the Class contributed to the security breach described herein or to the unauthorized access of their sensitive PII.

117. As a direct and proximate result of Defendant's misconduct described herein, Plaintiff and the Class were injured.

NINTH CAUSE OF ACTION
Negligence Per Se
(On behalf of Plaintiff and the Class)

118. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

119. Defendant's violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Cal. Penal Code § 502, Cal. Civ. Code §§ 1798.80, *et seq.*, and Cal. Civ. Code §§ 1750, *et seq.*, resulted in injury to Plaintiff and the Class.

120. The harm Defendant caused to Plaintiff and the Class are injuries that result from the type of occurrences those statutes were designed to prevent.

121. Plaintiff and the Class are the type of persons for whose protection those statutes were adopted.

122. Defendant's violations of the foregoing statutes as described herein resulted in injury to Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

A. Certify this case as a class action on behalf of the Class defined above, appoint Alan Claridge as class representative, and appoint his counsel as class counsel;

B. Declare that RockYou's actions, as described herein, violate the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*), the Computer Crime Law (Cal. Penal Code § 502), the California Security Breach Information Act (Cal. Civ. Code § 1798.80, *et seq.*), and the Consumer Legal Remedies Act (Cal. Bus. & Prof. Code § 1750).

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*: (i) an order prohibiting RockYou from engaging in the wrongful and unlawful acts described herein; and (ii) requiring RockYou to protect all data collected through the course of its business in accordance with industry standards;

D. Award damages, including statutory damages where applicable, to Plaintiff and the Class in an amount to be determined at trial;

E. Award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: December 28, 2009

By: _____
David Parisi
One of the Attorneys for Plaintiff